

UNITED STATES DISTRICT COURT

for the
Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Dropbox, Inc. account associated with email address
erndog82@gmail.com and stored at 1800 Owens St.,
Ste. 200 San Francisco, CA 94158

Case No. 1:20MJ147

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252A(a)(2)(A)	Distribution/Receipt of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

See Affidavit of Special Agent William D. Thompson.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ William D. Thompson

Applicant's signature

William D. Thompson, Special Agent (HSI)

Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date:

05/27/20

Judge's signature

City and state: Greensboro, North Carolina

The Honorable L. Patrick Auld, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information and data associated with the Dropbox, Inc. (Dropbox) account linked to email address erndog82@gmail.com, that is stored at premises owned, maintained, controlled, or operated by Dropbox, a company headquartered at 1800 Owens St., Ste. 200 San Francisco, CA 94158.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Dropbox, Inc. (Dropbox)

To the extent that the information described in Attachment A is within the possession, custody, or control of Dropbox, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to Dropbox, or have been preserved (**Dropbox preservation request, reference number CR-9000-00615**) pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All records or other information stored by an individual(s) using the account, including all images, videos, multimedia files and emails, stored and presently contained in, or preserved (**Dropbox preservation request, reference number CR-9000-00615**), or deleted, or on behalf of the account or identifier;
- b. All records or other information regarding the identification and subscriber of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the Internet protocol (IP) address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, mobile device information and means and source of payment (including any credit or bank account number);
- c. All transactional information of all activity of the Dropbox account, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting; and email "invites" sent or received via Dropbox, and any contacts list;
- d. All messaging logs, including date and time of messages, and usernames and/or email addresses sending and receiving correspondence;
- e. All records related to the types of services utilized;

- f. Billing records, showing all billable services;
- g. All records pertaining to communications between Dropbox and any person(s) regarding the account or identifier, including contacts with support services and records of actions taken;

Notwithstanding Title 18 U.S.C. § 2252 and Title 18 U.S.C. § 2252A, or any similar statute or code, Dropbox shall disclose responsive data by sending it to HSI Special Agent William Thompson at 140 Centrewest Court, Cary, North Carolina 27513 or via email to william.d.thompson@ice.dhs.gov.

II. Information to be seized by the government

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18 U.S.C. § 2252 and Title 18 U.S.C. § 2252A:

1. Child pornography, as defined in 18 U.S.C. 2256(8);
2. Child erotica;
3. Records, information, and items relating to violations of the statutes described above in the form of:
 - a. Records and information referencing child pornography, as defined in 18 U.S.C. 2256(8), and/or child erotica;
 - b. Records and information referencing or revealing the use of the handle "Eric Beal" or email address "erndog82@gmail.com" and any variants thereof, and the identity of the user;
 - c. Records and information referencing or revealing the owner or user(s) of the Dropbox account;
 - d. Records and information referencing or revealing the trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved and location of occurrence;
 - e. Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to

include the identity of the individuals involved and location of occurrence;

- f. Records and information referencing or revealing communication or interaction of an illicit sexual nature with minors, to include the identity of the individuals involved and location of occurrence;
- g. Records and information referencing or revealing participation in groups or the use of services that are known to be used to facilitate the trafficking of child pornography; and
- h. Records and information referencing or revealing the use of remote computing services such as email, cloud storage, or online social media services.

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH
WARRANT**

I, William D. Thompson, a Special Agent with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a warrant to search the Dropbox, Inc. (Dropbox) account associated with email address erndog82@gmail.com (hereinafter SUBJECT ACCOUNT). The SUBJECT ACCOUNT contents and information are stored at a Dropbox owned, maintained, controlled or operated premises. Dropbox is headquartered at 1800 Owens St., Ste. 200 San Francisco, CA 94158. This affidavit is made in support of an application for a search warrant under Title 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox to disclose to the government, records and other information in its possession, pertaining to the SUBJECT ACCOUNT.

2. I am investigating Ernie BRINN (BRINN) for distribution, receipt, and possession of child pornography, and I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B) are located within the SUBJECT ACCOUNT.

3. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located within the SUBJECT ACCOUNT.

AFFIANT BACKGROUND

4. I am a Special Agent of the U.S. Department of Homeland Security (DHS), HSI, formerly the United States Customs Service, having been so employed since December 2001, and I am currently assigned to the HSI Raleigh office in Cary, North Carolina. While employed by HSI, I have investigated federal criminal violations related to high technology and cybercrime, child exploitation, and child pornography. I have received training from the Federal Law Enforcement Training Center (FLETC) and other law enforcement agencies in the areas of child exploitation and pornography investigations and pedophile behavior. As part of my current duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production,

distribution, receipt and possession of child pornography. I have had the opportunity to observe and review numerous examples of child pornography as defined in Title 18 U.S.C. § 2256 in various forms of media, including computer media. In addition, I have participated in the execution of numerous search warrants involving child exploitation and child pornography offenses and I am in routine contact with experts in the fields of computers, computer forensics and Internet investigations.

STATUTORY AUTHORITY

5. As noted above, this investigation concerns violations of the following statutes:

- a. Title 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing child pornography, as defined in Title 18 U.S.C. § 2256(8), using any means and facility of interstate and foreign commerce, that has been mailed, or that has been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. Title 18 U.S.C. § 2252A(b)(1).
- b. Title 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in Title 18 U.S.C. § 2256(8), that has been mailed, shipped or transported using any means

or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. Title 18 U.S.C. § 2252A(b)(2).

BACKGROUND ON DROPBOX

6. Dropbox is a file hosting and sharing service operated by Dropbox which is headquartered in San Francisco, California, and is an electronic communication service, as defined in Title 18 U.S.C. § 2510(15), and/or a remote computer service, as defined in Title 18 U.S.C. § 2711(2). Dropbox offers cloud storage, file synchronization, personal cloud and client software to its users. Online storage mediums, such as Dropbox, make it possible for a user to access saved files without the requirement of storing said files on their own computer or other device. A Dropbox user can store digital files within a special folder on the user's device, and these files can be synchronized so the same folder with all the same digital content is accessible on each of the user's other devices which have the Dropbox application installed and synched with the user's account. Files placed in these folders may be accessed through the Dropbox website and through desktop and mobile device applications.

7. Dropbox users can share access to their digital files with others by

using the built-in option to create uniform resource locator (URL) hyperlinks to their Dropbox accounts ("links") and sending said links through email or social media accounts. Dropbox users can also allow others to upload and download digital files stored within specific shared folders in the user's account. Dropbox has desktop applications as well as mobile applications for Android, and iOS devices. Dropbox collects information like the user's name, email address, phone numbers, payment info, and physical address. Dropbox also collects IP addresses for the devices accessing the account, the type of browser, device used, as well as identifiers associated with the user's devices.

8. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

BACKGROUND ON KIK AND KIK REPORTS

9. Kik Messenger (Kik) is a mobile application designed for chatting or messaging. In October 2019, MediaLab, Inc., Santa Monica, California, purchased Kik from Ontario, Canada based Kik Interactive, Inc. According to

the publicly available document "Kik's Guide for Law Enforcement,"¹ to use this application, a user downloads the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an account and username. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can then send each other text messages, images, and videos.

10. According to "Kik's Guide for Law Enforcement," Kik users are also able to create chat groups with a limited number of individuals to communicate in a group setting and exchange text messages, images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a group name containing a hashtag (#) that is easily identifiable or searchable by keyword.

¹ Available at: <https://lawenforcement.kik.com/hc/en-us/categories/200320809-Guide-for-Law-Enforcement>.

11. According to information provided to HSI by a Kik Law Enforcement Response Team Lead, Kik's Terms of Service prohibit Kik users from uploading, posting, sending, commenting on, or storing content that contains child pornography and/or child abuse images. The Terms of Service also provide that Kik may review, screen and delete user content at any time if Kik believes use of their services are in violation of the law. According to Kik, Kik has a strong business interest in enforcing their Terms of Service and ensuring that their services are free of illegal content, and in particular, child sexual abuse material. Accordingly, Kik reports that it independently and voluntarily takes steps to monitor and safeguard their platform and that ridding Kik products and services of child abuse images is critically important to protecting their users, product, brand, and business interests.

12. Upon receipt of the information and evidence precipitating this search warrant application, and contained herein, Kik was in Ontario, Canada, and governed by Canadian law. According to information contained in the "Kik Interactive, Inc. Child Sexual Abuse and Illegal Material Report and Glossary" (Kik Glossary), which Kik provided when reporting information to law enforcement authorities, Kik was mandated to report to the Royal Canadian Mounted Police (RCMP) any images and/or videos that would constitute suspected child pornography under Canadian law which were discovered on the Kik platform. According to the Kik Glossary, Kik was typically alerted to

suspected child pornography on Kik based on digital hash value matches to previously identified child pornography or through reports from other Kik users or third-party moderators.

13. According to the Kik Glossary, Kik was mandated to report any images and/or videos that would constitute suspected child pornography which are discovered on the Kik platform. Furthermore, according to the Kik Glossary, Kik is typically alerted to suspected child pornography on Kik based on digital hash value matches to previously identified child pornography or through reports from other Kik users or third-party moderators.

14. According to the Kik Glossary, Kik has developed an internal hash matching system called "SafePhoto" (similar to Microsoft's PhotoDNA system) that Kik uses to scan images uploaded via Kik for suspected child pornography. Kik's SafePhoto database is comprised of hash values obtained from the International Criminal Police Organization (INTERPOL), the RCMP and the National Center for Missing and Exploited Children (NCMEC). Kik uses SafePhoto to run a hash value check against every image sent within Kik, including within private conversations, in order to detect images that may depict suspected child pornography and prevent such images from continuing to circulate through their application. When a user sends an image with a hash value that matches a child exploitation hash value in the SafePhoto database, Kik removes the content from its communications system, closes the user's

account and provides a SafePhoto report of the incident to the RCMP.

15. The RCMP advised HSI agents that upon receiving a report from Kik related to suspected child pornography, the RCMP reviewed the reported IP addresses of the Kik users contained in the Kik Reports to determine their location. The RCMP then provided Kik Reports of Kik users in the United States to HSI in Ottawa, Canada, who in turn provided the Kik Reports to the HSI Cyber Crimes Center (C3) Child Exploitation Investigations Unit (CEIU) located in Fairfax, Virginia for analysis and dissemination.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

16. In October 2019, HSI Raleigh received a Kik SafePhoto report referral from the C3 CEIU concerning Kik user "ericbeal2222" who was reported for Child Sexual Abuse and Illegal Material (CSAM). Within this SafePhoto report, Kik documented "ericbeal2222" uploaded and sent a suspected image of child pornography through their group chat platform. Kik identified this image was uploaded by "ericbeal2222" on May 2, 2019, at 05:12:08 Universal Time Coordinated (UTC) utilizing IP address 174.109.70.153.

17. As part of this referral, HSI Raleigh received an image from the HSI Cyber Crimes Center (C3). HSI C3 documented they located this image in C3's National Child Victim Identification System (NCVIS) database and it's hash value matched the hash value of the image uploaded by Kik user

"ericbeal2222" on May 2, 2019, at 05:12:08 UTC. I reviewed this image and verified it depicts child pornography showing a partially nude prepubescent female child. Within this image, the child is laying on her back on a carpeted floor and her right hand is touching her nude vaginal area which is positioned away from the camera. Also, at the fore of this image, a male's erect penis is visible and positioned on or near the child's left hand which she was holding on or near her mouth. In addition, a note reading, "I heart (a heart is drawn) CUM" was written on pink paper/material and positioned behind the child's head.

18. As part of this SafePhoto referral, HSI Raleigh also received Kik subscriber records and user information for "ericbeal2222." These records revealed this user identified his name as "Eric Beal," his birth date as October 20, 1979, and an email address, ericbeal222@yahoo.com, annotated by Kik as unconfirmed² and deactivated. In addition, Kik documented "ericbeal2222" utilized an iPhone to access his account.

19. On November 4, 2019, HSI Raleigh submitted a DHS Summons to ISP Charter Communications requesting subscriber information for IP address 174.109.70.153 on May 2, 2019, at 05:12:08 UTC. Charter Communications responded and identified the subscriber, on the requested date and time, as

² "Unconfirmed" means either that the email address is either invalid, or the user received a confirmation email from Kik but didn't click on the link to confirm.

Ernie Brinn at address 4524 Newby Drive, G1, Durham, North Carolina 27704.

20. Subsequent public records database queries related to Eric BEAL and email address ericbeal222@yahoo.com failed to reveal any relevant results or linkages to 4524 Newby Drive, G1, and Durham, North Carolina.

21. On or about October 10, 2019, HSI Raleigh conducted queries of the North Carolina Division of Motor Vehicles (DMV) and discovered Ernie BRINN's (DOB: July 28, 1970) active North Carolina driver license. Review of BRINN's driver license, which is scheduled to expire on July 28, 2026, revealed he provided 4524 Newby Drive, G1, Durham, North Carolina 27704 as his address.

22. On November 22, 2019, and January 17, 2020, I conducted vehicular surveillance and identified 4524 Newby Drive, G1, Durham, North Carolina 27704 as a first-floor apartment in a multi-unit building. 4524 Newby Drive, G1, Durham, North Carolina 27704 had a burgundy door with the numeral "1" posted on the white trim of the door. During surveillances, I observed a black Infiniti assigned North Carolina plate "ERND0G," registered to Ernie BRINN at 4524 Newby Drive, G1, Durham, North Carolina 27704, parked in the lot directly outside of 4524 Newby Drive, G1, Durham, North Carolina 27704.

23. On February 28, 2020, Magistrate Judge L. Patrick Auld issued

United States District Court, Middle District of North Carolina search and seizure warrant 1:20mj65 for 4524 Newby Drive, Apartment G1, Durham, North Carolina 27704 and 1:20mj66 for BRINN (date of birth (DOB) 07/28/1970).

24. On March 5, 2020, I and other law enforcement officers executed United States District Court, Middle District of North Carolina search and seizure warrants 1:20mj65 and 1:20mj66 at 4524 Newby Dr, G1, Durham, NC 27704.

25. On March 5, 2020, an on-scene preview of BRINN's Apple iPhone at 4524 Newby Drive, G1, Durham, North Carolina 27704 revealed a Dropbox account associated with email address erndog82@gmail.com and username Eric Beal, the same username reported by Kik for the individual who uploaded an illicit image of child pornography into their group chat platform, as previously documented within this affidavit, paragraphs 16 through 18.

26. On March 5, 2020, I submitted a preservation request(s) to Dropbox for the account associated with email address erndog82@gmail.com and username Eric Beal.

27. Based on my training and experience, as well as conversations with other law enforcement officers that investigate child exploitation cases, I know that individuals who use Kik Messenger to traffic in child pornography often store child pornography in Dropbox accounts for collection and sharing

purposes.

28. There is probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located within the SUBJECT ACCOUNT. Probable cause is based on the discovery of a Dropbox account on BRINN's iPhone which is registered to the same username, Eric Beal, which was used to register the Kik account utilized to upload an illicit image of child pornography into Kik's group chat platform.

INFORMATION REGARDING INFORMATION TO BE SEIZED

29. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular Title 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment A. Upon receipt of the information described in Section I of Attachment A, government-authorized persons will review that information to locate the items described in Section II of Attachment A.

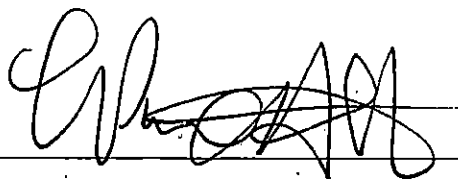
30. Because the warrant will be served on Dropbox who will then compile the requested records at a time convenient to Dropbox, reasonable cause exists to support execution of the requested warrant at any time day or night.

CONCLUSION

31. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by Title 18 U.S.C. § 2711, Title 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States ... that – has jurisdiction over the offense being investigated." Title 18 U.S.C. § 2711(3)(A)(i). Pursuant to Title 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

/s/ William D. Thompson *WDT*
William D. Thompson
Special Agent
Homeland Security Investigations

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which she submitted to me by reliable electronic means, on this 21st Day of May, 2020, at 4:51 pm.



L. PATRICK AULD

UNITED STATES MAGISTRATE JUDGE